TASK FORCE WEB

IT-21 Integration Considerations 9 July 2002

Mark Zabriskie
SPAWAR Systems Center San Diego
TFWeb IT21 Team

Agenda

- IT-21 Portal Installation.
- Configuration Management.
- Afloat to ashore connectivity.
- Shipboard Proxy Servers.
- Shipboard Application Configuration.

IT-21 Portal Installation

- The IT-21 portal environment includes the fleet Network Operations Centers (NOC) and every ship.
- Users in these environments use locally installed portals to access both local and remote (reach back) applications.

IT-21 Configuration Management

- In accordance with IT21 Configuration Management policy, each application owner will utilize the PPL, SSIL, QPL process for adding GOTS/COTS products to the Preferred Products List (PPL), Qualified Parts List (QPL), and System/Subsystem Interface List (SSIL).

Afloat to ashore connectivity

- Afloat to ashore connectivity often suffers from severe bandwidth limitations, and occasional outages.
- Biggest impact to reach-back applications.
- Monitor the CheckBandwidth property of the PRI Request for each connection.
- Consider the selection of different XSL style sheets on a per-connection basis to provide lightweight versions of UFS output.

Shipboard Proxy Servers.

- Each ship provides web proxies that require user authentication.
- Shipboard web access lists are driven by Information Control (INFOCON) and Operational Security Control (OPSECON) requirements.
- For varying levels of INFOCON and OPSECON, selective user groups are defined for off-ship web access and may restrict a significant number of ship users from web access.
- Application developers need to be aware of this limitation and design their applications accordingly.

Shipboard Application Configuration

- Each shipboard portal will synchronize the Service Registry with the shore portals on a periodic basis.
- A UFS that has any dependencies on specific ships, or ship types will need to provide a list of designated ships in the registration metadata, “Target Portals”.

TASK FORCE WEB

Mobile Code Hosting 09 July 2002

Mark Zabriskie
SPAWAR Systems Center San Diego
TFWeb IT21 Team

Mobile Code Hosting

- DoD Mobile Code Policy restricts the delivery of mobile code between enclaves.
- We can assist you with compliance and provide a host platform for code modules. This may not be an issue with your application, review the policy.
- Mobile Code modules need to be submitted and certified, similar to other applications.
- The Service Registry provides a listing of currently certified and hosted code modules.
- The target server must be defined as a "trusted site" in the browser settings.

Mobile Code Reference

- Code modules will be hosted at a designated URL:

  https://www.homeport.navy.mil/mobilecode/module.ocx

- Application references to code modules need to be updated. An ActiveX control might be referenced in HTML as:

```
<OBJECT
ALIGN=CENTER CLASSID="clsid:99B42120-6EC7-11CF-A6C7-00AA00A47DD2"
WIDTH=200 HEIGHT=200 ID=MyObject
CODEBASE="https://www.homeport.navy.mil/mobilecode/module.ocx#ver=4,
70,0,1062">
  <PARAM NAME="ScrollStyleX" VALUE="Circular">
</OBJECT>
```

TASK FORCE WEB

Migration of Pilot Service Modules
09 July 2002

Mark Zabriskie
SPAWAR Systems Center San Diego
TFWeb IT21 Team

Pilot Service Modules

- Issue: Your application was in the pilot of the NEP.
  - You have a “Service Module”. What happens next?
- Answer:
  - Service Modules are no longer used.
  - You have options:
    1. Move the Service Module to your application backend. This may be the simplest path for prior Level 1 and Level 3 Service Modules. However… updated PRI data may impact your existing Service Module design
    2. You may wish to develop a new UFS that takes advantage of updated portal features.
  - You need to provide updated application registration metadata to us.
  - We will re-test your application in the portal